Vivid Risk



BOARD BRIEFING PACK

Cyber Risk, NIS2, DORA, GDPR & the NIS Regulations

A practical framework for boards in Ireland, the UK and the EU

Boards now answer for cyber and data-protection risk. This pack sets out a three-step way to meet that responsibility (assess, prioritise, govern) and shows what the Vivid Risk platform gives a board at each step, and what it does not do.

THE BOARD'S POSITION

Cyber risk is a board-level responsibility

The rules that apply depend on where you operate and what you do, but they share one idea: **the people who run the organisation are answerable for how it manages cyber and data-protection risk**. That duty sits with the management body, not with the IT team or the providers it relies on.

NIS2

EU MEMBER STATES

Management bodies approve the cybersecurity risk-management measures, oversee their implementation, can be held liable, and must follow training (Art. 20).

DORA

EU FINANCIAL ENTITIES

The management body bears ultimate responsibility for managing the entity's ICT risk (Art. 5).

NIS Regulations 2018

UK · IRELAND

The UK is not under NIS2: its NIS Regulations and the NCSC CAF apply. Ireland has not yet transposed NIS2, so S.I. No. 360/2018 still applies.

GDPR

EU · UK GDPR

The controller must implement appropriate measures and be able to demonstrate that processing complies (Art. 24).

The hard part is visibility. Boards usually learn the state of their security from the people and providers they are meant to oversee, in the form of policies, certificates and assurances. What they rarely get is a structured, control-by-control picture they can question, track over time and act on.

> **A board cannot oversee what it cannot see.**

THE RECOMMENDED APPROACH

A board-ready framework: Assess. Prioritise. Govern.

1 STEP 01

Assess

Answer a structured self-assessment and get a maturity score, with each scored control cited against the frameworks that apply where you operate.

2 STEP 02

Prioritise

Turn the gaps into a ranked list: reporting duties and severe gaps first, then what each fix recovers, with owners and a budget you set.

3 STEP 03

Govern

Track progress across reassessments, keep evidence beside the answers, and be ready for the incident-reporting deadlines before you need them.

Vivid Risk is a self-assessment platform. It does not audit you, test your systems or file anything with a regulator. It gives your board, your team and your advisers one structured picture to work from.

WHAT SITS BEHIND THE FRAMEWORK

What the board receives at every stage

Vivid Risk

ASSESS — PRIORITISE — GOVERN

01

ASSESS

Maturity Assessment & Vivid Maturity Index

A structured questionnaire covering governance, identity and access, endpoints, networks, data, suppliers and resilience. Answers are scored into the Vivid Maturity Index (VMI) on a five-tier scale from Initial to Optimized; "not applicable" answers leave the score rather than count against you.

You receive: your VMI and tier, a findings report with severe gaps flagged as critical, a full report and a response log; at a VMI of 90+ with no severe gap, a Certificate of Diligence (not an audit or an accredited certification).

Cited against · NIS2 Art. 21 & 23 (EU) · NCSC CAF v4.0 (UK) · ISO 27001 Annex A · NIST CSF 2.0 · GDPR

02

ASSESS

Evidence Beside Every Answer

Upload the documents behind your answers; each shows how fresh it is, and changes are kept in a tamper-evident record. One read-only connection (Google Workspace) places counts beside your answers; it never answers a control for you.

You receive: an ISO 27001 audit pack for your auditor and, on higher plans, an AI cross-map of your documents against the frameworks, marked as an AI-generated draft for review.

Supports · ISO 27001 · NIS2 · DORA · GDPR accountability

03

PRIORITISE

Start Here: a Ranked Top Ten

Findings become decisions. Gaps that touch a reporting duty or a severe control come first, then the rest by how much score each fix recovers. Each action gets a window: immediate (30 days), next 90 days, or planned (180 days).

You receive: a "Start here" PDF of the ten actions to take first and a prioritised action list for the whole assessment.

Ranks by · reporting duty · severity · score recovered

04

PRIORITISE

Remediation Queue & Budget Plan

Assign each gap to a named owner, log the effort and attach the evidence that closes it. Enter what each fix costs and the budget optimiser picks the fixes that recover the most score within your budget. The costs are yours; the product does not estimate them.

You receive: a remediation queue with owners and status, a roadmap action plan in the full report, and a budget-constrained shortlist.

Tied to · the control and framework citations behind each gap

05

GOVERN

Incident Reporting Clocks

Log an incident and the platform shows every reporting clock that applies and when each report is due. It records what you file; it files nothing with any authority.

You receive: an incident register with deadlines for NIS2 (24h / 72h / 1 month), DORA (4h after classification, no later than 24h after awareness, then 72h and 1 month), GDPR and UK GDPR (72h), the UK and Irish NIS Regulations (72h) and CRA Art. 14.

Cited against · NIS2 Art. 23 · DORA Art. 19 · GDPR Art. 33 · NIS Regs 2018 · CRA Art. 14

06

GOVERN

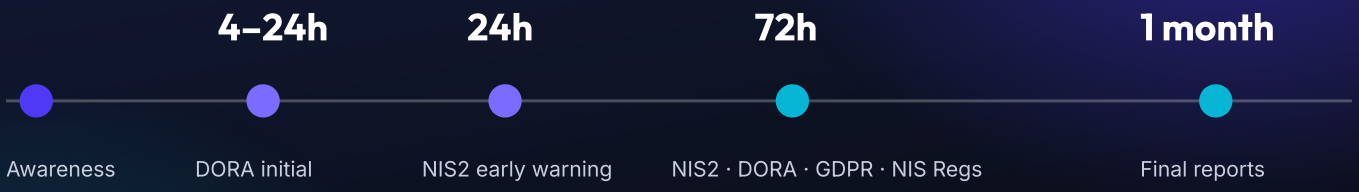
Executive Views & Third-Party Register

Views for the CEO, CTO, compliance and risk leads from the same assessment, with score trends across reassessments; and a register of your suppliers, showing where too much depends on one provider.

You receive: role-based executive views, a supplier register you maintain, and, for DORA entities, a draft Register of Information export (4 of the 15 templates, as CSV).

Relates to · DORA Art. 28 (third-party risk) · GDPR Art. 28

WHEN AN INCIDENT STARTS THE CLOCK



Which deadlines apply depends on your sector and jurisdiction. Shown for illustration; the register applies the rules for your case.

WHERE DOES YOUR BOARD STAND TODAY?

Three questions every board should be able to answer

01 Do we know which rules apply to us (NIS2, the NIS Regulations, DORA, GDPR) and which reporting deadlines start the moment an incident happens?

02 Can we show, control by control, where we stand today and what evidence sits behind each answer?

03 Do we know which gaps to close first, who owns each one, and what it will cost?

If the answer to any of these is uncertain, that is where the assessment starts.

What Vivid Risk is not

The platform is a self-assessment, not an audit or a certification. It does not test your systems, monitor them, or file anything with a regulator. When you need independent testing or an audit, our provider directory (vividrisk.ai/providers) lists auditors, managed-service providers and consultancies; Vivid Risk does not assess or endorse them, and the choice is yours.

TALK TO US

Request a walkthrough for your board

We will take you through the assessment, the reports your board receives and how the reporting clocks apply to your organisation.

Hussam Ismail
Director, Vivid Risk LTD

info@vividrisk.ai
vividrisk.ai

Vivid Risk

Vivid Risk LTD · Company registration number 818204 (Ireland)
Based in Dublin, Ireland
Assess risk, stay audit-ready, and simplify compliance.